Lori G. Feldman (*pro hac vice* forthcoming)
GEORGE FELDMAN MCDONALD, PLLC
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Telephone: (917) 983-9321
Email: lfeldman@4-justice.com

David J. George (*pro hac vice* forthcoming)
Brittany Brown (*pro hac vice* forthcoming)
GEORGE FELDMAN MCDONALD, PLLC
9897 Lake Worth Road, Suite 302
Lake Worth, FL 33467
Telephone: (561) 232-6002
Email: dgeorge@4-justice.com
bbrown@4-justice.com

THE WAND LAW FIRM, P.C.
Aubry Wand (SBN 281207)
100 Oceangate, Suite 1200
Long Beach, CA 90802
Telephone: (310) 590-4503
Email: awand@wandlawfirm.com

Attorneys for Plaintiff and the Putative Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

JANE DOE, individually and on behalf of all others similarly situated,

Plaintiff,

v.

CEREBRAL, INC., a Delaware corporation; and DOES 1 through 10, inclusive,

Defendant.

CASE NO.:

CLASS ACTION COMPLAINT

1. Negligence
2. Negligence *Per Se*
3. Breach of Implied Contract
4. Breach of Implied Covenant of Good Faith and Fair Dealing
5. Breach of Fiduciary Duty
6. Breach of Confidence
7. Declaratory Judgment
8. Unjust Enrichment

DEMAND FOR JURY TRIAL

Plaintiff Jane Doe ("Plaintiff"), on behalf of herself and all others similarly situated, alleges as and for her Class Action Complaint, the following against Cerebral Inc. ("Cerebral," the "Company," or "Defendant"), based upon her personal knowledge with respect to herself and her own acts, and upon information and belief, upon her own investigation and the investigation of her counsel, as to all other matters, as follows:

I. INTRODUCTION

1. Confidentiality is a fundamental and critical aspect of mental healthcare. It is essential for the free flow of information between patients and their therapists. When confidentiality is compromised, so is trust. Millions of Americans provided highly sensitive and confidential information regarding themselves and their mental health to Cerebral and trusted that the Company would appropriately safeguard it. This class action seeks to hold Cerebral accountable for its egregious, unlawful breaches of the privacy of Plaintiff and members of the proposed class.

2. Cerebral is an online mental health subscription service that provides its customers with ongoing access to online mental health care and mental health medication management for a monthly charge. The Company provides its services remotely, utilizing telehealth technology to provide online therapy and medication management for various mental health conditions, including anxiety, depression, ADHD, bipolar disorder, borderline personality disorder, and substance abuse, among others. Cerebral's customers are patients who reside throughout the United States ("Patients").

3. This class action arises from Cerebral's negligent, reckless, and/or intentional failure to implement and maintain adequate data protection, resulting in the unlawful disclosure of highly sensitive personal and medical information of Cerebral's customers to third parties, which was discovered by Cerebral on or around January 3, 2023, and publicly acknowledged by Cerebral on or around March 1, 2023 ("the Privacy Breach"). Plaintiff brings this action on behalf citizens

of all states in the United States whose information was disclosed through the Privacy Breach (the "Class" and "Class Members").[1]

4. According to Cerebral's privacy breach notice, Cerebral determined on January 3, 2023 that it had had disclosed certain information that may be regulated as protected health information under HIPAA to certain "Third-Party Platforms and some Subcontractors without having obtained HIPAA-required assurances."[2]

5. According to Cerebral, the Privacy Breach stemmed from Cerebral's use of what are called "pixels" and similar tracking technologies, such as those made available by Google, Meta (Facebook), TikTok, and other third parties.[3]

6. On March 1, 2023, Cerebral reported on the U.S. Department of Health and Human Services breach portal that 3,179,835 people had their information exposed as part of the Privacy Breach.

7. As a healthcare provider, Cerebral knowingly collected Members' personally identifiable information ("PII"), and protected health information ("PHI") (collectively, "Private Information") in confidence, and has a resulting duty to secure, maintain, protect, and safeguard that Private Information against unauthorized access and disclosure through reasonable and adequate security measures.

8. PHI is considered "the most confidential and valuable type of [PII], irrevocable once breached."[4]

9. As a result of the Privacy Breach, Plaintiff and Class Members suffered ascertainable losses, including but not limited to, a diminution in the value of their

---

[1] Notice of HIPAA Privacy Breach, available at https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last accessed March 16, 2023).

[2] *Id.*

[3] *Id.*

[4] Junyuan Ke et al, My Data or My Health? Heterogenous Patient Responses to Healthcare Data Breach (February 2, 2022), available at: http://dx.doi.org/10.2139/ssrn.4029103 (last accessed March 16, 2023).

private and confidential information, the loss of the benefit of their contractual bargain with Defendant, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the Privacy Breach.

10. Plaintiff's and Class Members' sensitive and private personal information— entrusted to Defendant, its officials, and agents—was unlawfully shared with third party platforms in the Privacy Breach. Information compromised in the Privacy Breach includes: full names, telephone numbers, email addresses, dates of birth, IP addresses, Cerebral client ID number, demographic information, confidential self-assessment responses and associated health information, subscription plan type, appointment dates, treatment details and other clinical information, and health insurance/pharmacy benefit information, as well as other Private Information and protected health information defined by HIPPA.[5]

11. This information was leaked to third parties from October 12, 2019 through March 6, 2023, when the company disabled the tracking pixels.[6]

12. Plaintiff brings this class action lawsuit on behalf of all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information, for failing to provide timely and adequate notice to Plaintiff and other Class Members of the unauthorized access to their Private Information by an

[5] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.* ("HIPAA"), PHI is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, *available at*: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed March 16, 2023).

[6] *See, e.g.*, https://www.bleepingcomputer.com/news/security/mental-health-provider-cerebral-alerts-31m-people-of-data-breach/ (last accessed March 16, 2023).

unknown third-party, and for failing to provide timely and adequate notice of precisely what information was accessed and unlawfully shared.

13. Defendant breached its duty to Plaintiff and Class Members by maintaining Plaintiff's and the Class Members' Private Information in a negligent, reckless, and/or intentional manner.

14. Upon information and belief, the means of the Privacy Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information were known and foreseeable risks to Defendant. Thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left the Private Information in a dangerous and vulnerable condition.

15. Defendant and its employees failed to properly monitor its computer technology for the tracking devices.

16. Had Defendant properly adequately monitored its technology, it would have discovered the trackers sooner or been able to wholly prevent them from tracking in the first instance.

17. Exacerbating an already devastating privacy intrusion, Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent, reckless and/or intentional conduct since the Private Information that was tracked and is now in the hands of unauthorized third parties.

18. Armed with the Private Information accessed in the Privacy Breach, unauthorized third parties have data from Cerebral to commit a variety of unlawful acts, including credit/debit card fraud, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical/mental health services, utilizing the Private Information to blackmail Patients who thought their highly-personal mental health data would be kept in the strictest of confidence, using Class Members' health information to target other phishing and hacking intrusions based upon their individual health needs, using Class Members' information to obtain government benefits, filing

fraudulent tax returns using Class Members' information, and obtaining driver's licenses in Class Members' names but with another person's photograph.

19. As a direct result of the Privacy Breach, Plaintiff and Class Members have suffered loss of their highly personal and confidential mental health records – and continue to be exposed to a heightened and imminent risk of reputational damage, healthcare and other fraud, and identity theft, potentially for the rest of their lives. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

20. As a direct and proximate result of the Privacy Breach and subsequent exposure of their Private Information, Plaintiff and Class Members have suffered, and will continue to suffer, damages and economic losses in the form of lost time needed to take appropriate measures to avoid unauthorized and fraudulent charges, dealing with loss of employment and/or reputational damage, putting alerts on their credit files, and addressing spam messages and e-mails received as a result of the Privacy Breach. Plaintiff and Class Members have suffered, and will continue to suffer, an invasion of their property interest in their own PII and PHI such that they are entitled to damages from Defendant for unauthorized access to, theft of, and misuse of their PII and PHI. These harms are ongoing, and Plaintiff and Class Members will suffer from future damages associated with the unauthorized use and misuse of their PII and PHI as unauthorized third parties will continue to use the information to obtain money, credit, fraudulent healthcare, in their names, and also cause unseemly reputational damage to Patients, for years to come.

21. Plaintiff seeks to remedy these harms on behalf of all similarly situated individuals whose Private Information was accessed and/or removed from Defendant's network during the Privacy Breach.

22. Accordingly, Plaintiff brings this action, on behalf of herself and all others similarly situated, against Defendant seeking redress for its unlawful conduct asserting claims for negligence, negligence *per se*, breach of express contract,

breach of implied contract, breach of the implied covenant of good faith and fair dealing, negligent misrepresentation, invasion of privacy by intrusion, breach of fiduciary duty, breach of confidence, declaratory judgment, and unjust enrichment.

II. PARTIES

23. Plaintiff Jane Doe ("Plaintiff Doe") is a resident of Cook County, Illinois. Plaintiff Doe is a Cerebral Patient and a monthly subscriber of the Company's services. She reviewed the Company's notice stating that her Private Information was improperly exposed to unauthorized third parties by Cerebral.

24. Defendant Cerebral is a Delaware corporation with its principal place of business in Walnut, California. Cerebral offers a telehealth platform that gives access to monthly mental health and wellness support, including online therapy, mental health assessments and expert care through behavioral health coaching, talk therapy, medication management, and personalized content. Cerebral serves patients throughout the United States.

III. JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and there are thousands of members of the class that are citizens of states different from Defendant.

26. This Court has personal jurisdiction over Defendant because Cerebral is headquartered in the State of California, its principal place of business is in California, and it regularly conducts business in California.

27. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendant resides in this District, a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in, was directed to, and/or emanated from this District, Cerebral is based in this District, Cerebral maintains

Members' Private Information in this District, and Defendant has caused harm to Plaintiff and Class Members residing in this District.

IV. STATEMENT OF FACTS

A. Cerebral's Business.

28. Due to the nature of its healthcare services, Cerebral must store Members' Private Information and Private Health Information in its computer systems. Cerebral accomplishes this by keeping the PII and PHI electronically, as evidenced by this Privacy Breach.

29. Members demand and are entitled to security to safeguard their Private Information. As a healthcare provider, Cerebral is required to ensure that such private, personal information is not disclosed or disseminated to unauthorized third parties without Members' express, written consent, as further detailed below.

B. The Privacy Breach.

30. On January 3, 2023, Cerebral determined that it had disclosed certain information that may be regulated as protected health information under HIPAA to certain third-party platforms and some subcontractors without having obtained HIPAA-required clearances. Due to a tracking pixel's data logging features, Cerebral stated that the confidential and sensitive medical information of people who used the provider's platform was exposed to third parties without the patient's permission.

31. According to Cerebral's privacy breach notice, Cerebral determined on January 3, 2023, that it had had disclosed certain information that may be regulated as protected health information under HIPAA to certain "Third-Party Platforms and some Subcontractors without having obtained HIPAA-required assurances."[7]

[7] *Id.*

32. According to Cerebral, the Privacy Breach stemmed from Cerebral's use of what are called "pixels" and similar tracking technologies, such as those made available by Google, Meta (Facebook), TikTok, and other third parties.[8]

33. On March 1, 2023, Cerebral reported on the U.S. Department of Health and Human Services breach portal that 3,179,835 people had their information exposed as part of the Privacy Breach.

34. On its website, Cerebral assures Class Members: "We use the latest information security technology to protect your data, which is not shared without your consent, and will only be used internally to improve clinical care."

35. Cerebral issued a Notice of HIPAA Privacy Breach on its website informing Patients of the Privacy Breach ("Notice") beginning in March 2023.

C. Plaintiff's Experiences Following the Privacy Breach.

Plaintiff Jane Doe

36. Plaintiff Doe subscribed to Cerebral and paid for her subscription on a monthly basis at all times relevant to this action.

37. Plaintiff Doe's PII and PHI was available to Cerebral through her status as a medical patient.

38. As a result of the Privacy Breach, Plaintiff has suffered emotional distress as a result of the release of her protected health information which she expected Cerebral to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using her personal and medical information.

39. Plaintiff Doe suffered actual injury from having her Private Information exposed as a result of the Privacy Breach including, but not limited to (a) paying monies to Cerebral for its services which she would not have paid had Cerebral disclosed that it lacked data security practices adequate to safeguard

[8] *Id.*

patients' Private Information from theft; (b) damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff entrusted to Cerebral as a condition for healthcare services; (c) loss of her privacy; and (d) imminent and impending injury arising from the increased risk of fraud and identity theft.

40. As a result of the Privacy Breach, Plaintiff Doe will continue to be at heightened risk for financial fraud, medical fraud and identity theft, and the attendant damages, for years to come.

D. Cerebral's Privacy Policies.

41. As stated above, on its website Cerebral states: "We use the latest information security technology to protect your data, which is not shared without your consent, and will only be used internally to improve clinical care."

42. By failing to protect Plaintiff's and Class Members' Private Information, and by allowing the Privacy Breach to occur, Cerebral broke these promises to Plaintiff and Class Members.

E. Cerebral Acquires, Collects and Stores Its Members' Private Information.

43. Cerebral acquires, collects, and stores a massive amount of its Patients' PHI and PII.

44. As a condition of engaging in mental healthcare, Cerebral requires that these Members entrust it with their highly confidential Private Information.

45. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Cerebral assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

46. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information, and, as current and former Patients, they relied on Cerebral to keep this information confidential and securely

maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

F. The Value of Private Information and the Effects of Unauthorized Disclosure.

47. At all relevant times, Defendant was aware that the Private Information it collects from Plaintiff and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

48. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[9] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

49. While credit card information and associated PII can sell for as little as $1-$2 on the black market, PHI can sell for as much as $363 according to the Infosec Institute.[10]

50. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

51. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or

---

[9] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed March 16, 2023).

[10] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at*: https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last accessed March 16, 2023).

mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[11]

52. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

53. The ramifications of Cerebral's failure to keep its Patients' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

54. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

55. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[12] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they

[11] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last visited March 16, 2023).

[12] *See* Medical ID Theft Checklist, available at: https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last accessed March 7, 2023).

received collection letters from creditors for expenses that were incurred in their names.[13]

56. As a healthcare provider, Cerebral knew, or should have known, the importance of safeguarding its Patients' Private Information entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Cerebral's Patients due to the breach. Cerebral failed, however, to take adequate cybersecurity measures to prevent the Privacy Breach from occurring.

G. Cerebral's Conduct Violates HIPAA.

57. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[14]

58. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

59. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual

[13] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages"), available at*: https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-ealthcare.pdf (last accessed March 7, 2023).

[14] HIPAA Journal, *What is Considered Protected Health Information Under HIPAA?, available at*: https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/ (last accessed March 7, 2023).

"without unreasonable delay and in no case later than 60 days following discovery of the breach."[15]

60. Based on information and belief, Defendant's Privacy Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. Cerebral's security failures include, but are not limited to, the following:

i. Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

ii. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

iii. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);

iv. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

v. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2);

vi. Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

vii. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. §164.306(a)(94);

viii. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, et seq.;

[15] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last visited March 7, 2023).

ix. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

x. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

H. Cerebral Failed to Comply with FTC Guidelines.

61. Cerebral was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

62. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[16]

63. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[17] The guidelines note that businesses should protect the personal

[16] Federal Trade Commission, *Start With Security: A Guide for Business, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed March 7, 2023).

[17] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed March 7, 2023).

customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

64. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

65. The FTC has brought enforcement actions against businesses for failing to adequately protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

66. Cerebral failed to properly implement basic data security practices. Cerebral's failure to employ reasonable and appropriate measures to protect against unauthorized access to Patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

67. Cerebral was at all times fully aware of its obligation to protect the Private Information of Patients because of its position as a trusted healthcare provider. Cerebral was also aware of the significant repercussions that would result from its failure to do so.

///

///

///

///

I. Cerebral Failed to Comply with Healthcare Industry Standards.

68. HHS's Office for Civil Rights notes:

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations, as they store large quantities of highly Private and valuable data.[18]

69. HHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training healthcare employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

70. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because of the value of the Private Information which they maintain and because as an industry they have been slow to adapt and respond to cybersecurity threats.[19] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of Private Information.

71. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, Cerebral chose to ignore them. These best practices were known, or should have been known, by Cerebral, whose failure to heed and properly implement them directly led to the Privacy Breach and the unlawful exposure of Class Members' Private Information.

---

[18] HIPAA Journal, Cybersecurity Best Practices for Healthcare Organizations, https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/ (last accessed March 16, 2023).

[19] *See, e.g.*, INFOSEC, *10 Best Practices For Healthcare Security*, *available at*: https://resources.infosecinstitute.com/category/healthcare-information-security/is-best-practices-for-healthcare/10-best-practices-for-healthcare-security/#gref (last accessed March 16, 2023).

J. Unauthorized Third Parties Have and Will Continue to Use Plaintiff's and Class Members' Private Information for Nefarious Purposes.

72. Plaintiff's and Class Members' highly sensitive Private Information is of great value to unauthorized third parties. and the data released in the Privacy Breach can be used in a variety of ways to exploit Plaintiff and Class Members and to profit off their misfortune and disclosed information.

73. Every year, identity theft causes tens of billions of dollars of losses to victims in the United States.[20] For example, with the Private Information released in the Privacy Breach, including Social Security numbers and financial information, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[21] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members

74. Third parties may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding Privacy Breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.

---

[20] Facts + Statistics: Identity Theft and Cybercrime, Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity") (last accessed on March 16, 2023).

[21] *See, e.g.*, Christine DiGangi, 5 Ways an Identity Thief Can Use Your Social Security Number, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-anidentity-thief-can-do-with-your socialsecurity-number-108597/ (last accessed March 16, 2023).

As a result, studies that attempt to measure the harm resulting from Privacy Breaches cannot necessarily rule out all future harm.[22]

75. For instance, with a stolen Social Security number, which is part of the PII compromised in the Privacy Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[23]

76. If unauthorized third parties manage to access financial information, health and medical information, and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may expose the Plaintiff and Class Members.

K. Plaintiff and Class Members Suffered Damages.

77. The ramifications of Cerebral's failure to keep Members' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of Privacy Breaches are more likely to become victims of identity fraud.[24]

78. In addition to their obligations under state laws and regulations, Defendant owed a common law duty to Plaintiff and Class Members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private

[22] Stolen Laptops Lead to Important HIPAA Settlements, U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archiveit.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolenlaptops-lead-to-important-hipaa-settlements.html (last accessed March 16, 2023).

[23] *See, e.g.*, Christine DiGangi, 5 Ways an Identity Thief Can Use Your Social Security Number, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-anidentity-thief-can-do-with-your-socialsecurity-number-108597/ (last accessed March 16, 2023).

[24] *2014 LexisNexis True Cost of Fraud Study, available at*: https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed March 16, 2023).

Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

79. Defendant further owed and breached its duty to Plaintiff and Class Members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

80. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Privacy Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse to Plaintiff's and Class Members' Private Information as detailed above, and Plaintiff is now at a heightened and increased risk of identity theft and fraud.

81. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record, especially if Class Members' mental health records such as treatment plans, diagnoses, and medication are disclosed. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

82. Other risks of identity theft include loans opened in the name of the victim, medical services billed in their name, utility bills opened in their name, tax return fraud, and credit card fraud.

83. Plaintiff and Class Members did not receive the full benefit of the bargain, and instead received mental healthcare services that were of a diminished value to that described in their agreements with Cerebral and they were damaged in an amount at least equal to the difference in the value of the mental healthcare with the data security protection they paid for and the mental healthcare they received.

84. As a result of the Privacy Breach, Plaintiff's and Class Members' Private Information has diminished in value.

85. The Private Information belonging to Plaintiff and Class Members is private, private in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standards.

86. The Privacy Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

87. Defendant had the resources necessary to prevent the Privacy Breach, but neglected to adequately implement data security measures, despite its obligation to protect Members' data.

88. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiff's and Class Members' Private Information.

89. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Privacy Breach on their lives.

90. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[25]

91. Defendant's failure to adequately protect Plaintiff's and Class Members' Private Information has resulted in Plaintiff and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money – while Defendant sits by and does nothing to assist those affected by the incident. Instead, as Cerebral's Privacy Breach Notice indicates, it is putting the burden on Plaintiff and Class Members to discover possible fraudulent activity and identity theft.

92. As a result of Defendant's failures to prevent the Privacy Breach, Plaintiff and Class Members have suffered, will suffer, and are at increased risk of suffering:

i. The compromise, publication, theft and/or unauthorized use of their Private Information;
ii. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
iii. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Privacy Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
iv. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession;
v. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of

[25] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012, December 2013, available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed March 16, 2023).

the Privacy Breach for the remainder of the lives of Plaintiff and Class Members; and

vi. Anxiety and distress resulting from fear of misuse of their medical information.

93. In addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

V. CLASS ALLEGATIONS

94. Plaintiff brings this class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

95. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **Nationwide Class: All individuals whose Private Information was compromised in the Cerebral Privacy Breach from October 12, 2019 to March 6, 2023.**

96. Excluded from the Nationwide Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, current or former employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

97. Plaintiff reserves the right to modify or amend the definition of the proposed Nationwide Class before the Court determines whether certification is appropriate.

98. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class is so numerous that joinder of all members is impracticable. Defendant has identified more than 3,000,000 patients whose Private Information may have been improperly accessed in the Privacy Breach whose Private Information was compromised, and the Nationwide Class is apparently identifiable within Defendant's records.

99. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Nationwide Class exist and predominate over any questions affecting only individual Class Members. These include:

i. Whether and when Defendant actually learned of the Privacy Breach and whether its response was adequate;

ii. Whether Defendant owed a duty to the Nationwide Class to exercise due care in collecting, storing, safeguarding and/or obtaining their Private Information;

iii. Whether Defendant breached that duty;

iv. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class Members' Private Information;

v. Whether Defendant acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class Members' PII/PHI;

vi. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class Members' PII/PHI secure and prevent loss or misuse of that Private Information;

vii. Whether Defendant caused Plaintiff's and Class Members' damages;

viii. Whether Defendant violated the law by failing to promptly notify Members of the Nationwide Class that their Private Information had been compromised;

ix. Whether Plaintiff and the other Class Members are entitled to actual damages, credit monitoring, and other monetary relief; and

x. Whether Defendant violated common law and statutory claims alleged herein.

100. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members, because all had their Private Information compromised as a result of the Privacy Breach, due to Defendant's misfeasance.

101. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Nationwide Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Nationwide Class and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect the Nationwide Class uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Nationwide Class as a whole, not on facts or law applicable only to Plaintiff.

102. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Nationwide Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Nationwide Class and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

103. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large

number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

104. The nature of this action and the nature of laws available to Plaintiff and the Nationwide Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Nationwide Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited resources of each individual Member of the Nationwide Class with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Nationwide Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

105. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of the Members of the Nationwide Class demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

106. Adequate notice can be given to Members of the Nationwide Class directly using information maintained in Defendant's records.

107. Unless a Class-wide injunction is issued, Plaintiff and Class Members remain at risk that Defendant will continue to fail to properly secure the Private Information of Plaintiffs and the Nationwide Class resulting in another Privacy Breach, continue to refuse to provide proper notification to Class Members regarding the Privacy Breach, and continue to act unlawfully as set forth in this Complaint.

108. Defendant has acted or refused to act on grounds generally applicable to the Nationwide Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Nationwide Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

109. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

i. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and safeguarding their Private Information;

ii. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

iii. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

iv. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Privacy Breach; and

v. Whether Class Members are entitled to actual damages, additional credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

COUNT I

NEGLIGENCE

(On Behalf of Plaintiff and the Nationwide Class)

110. Plaintiff repeats and realleges all allegations set forth in paragraphs 1 through 109 above as if they were fully set forth herein.

111. Defendant required Plaintiff and Class Members to submit PII and PHI to obtain online mental healthcare services.

112. Defendant knew, or should have known, of the risks inherent in collecting and storing the PII and PHI of Plaintiff and Class Members.

113. As described above, Defendant owed duties of care to Plaintiff and Class Members whose PII and PHI had been entrusted with Cerebral.

114. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate protection to safeguard Plaintiff's and Class Members' PII and PHI.

115. Defendant acted with wanton disregard for the confidentiality of Plaintiff's and Class Members' PII and PHI. Defendant knew or should have known that Cerebral was incapable of adequately storing, maintaining, and maintaining the highly confidential nature of Class Member's information in light of the pixel and tracking technology being utilized on its computer systems.

116. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Cerebral entered into a "special relationship" with Plaintiff and Class Members because Cerebral collected the PII and PHI of Plaintiff and the Class Members and stored it in the Cerebral Database –information that Plaintiff and the Class Members had been required to provide to Cerebral.

117. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and the Class Members, Plaintiff and the Class Members would not have been injured.

118. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known it was failing to meet its duties, and that Defendant's breach of such duties would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII and PHI.

119. As a direct and proximate result of Defendant' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II

Negligence *Per Se*

(On behalf of Plaintiff and the Nationwide Class)

120. Plaintiff repeats and realleges all allegations set forth in paragraphs 1 through 109 above as if they were fully set forth herein.

121. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and PHI.

122. Pursuant to HIPAA (42 U.S.C. § 1302d *et. seq.*), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' PII and PHI.

123. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45) and HIPAA (42 U.S.C. § 1302d *et. seq.*), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and PHI.

124. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

125. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

126. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII and PHI.

127. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III

Breach of Implied Contract

(On behalf of Plaintiff and the Nationwide Class)

128. Plaintiff repeats and realleges all allegations set forth in paragraphs 1 through 109 above as if they were fully set forth herein.

129. Plaintiff and Class Members entered into an implied contract with Cerebral when they obtained mental healthcare services from Cerebral, for which they were required to provide their PII and PHI. The PII and PHI provided by Plaintiff and Class Members to Cerebral was governed by and subject to Cerebral's privacy duties and policies.

130. Cerebral agreed to safeguard and protect the PII and PHI of Plaintiff and Class Members and to timely and accurately notify them if their PII or PHI was compromised.

131. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that Defendant's data protection practices and policies were reasonable and consistent with industry standards. Plaintiff and Class Members

believed that Cerebral would use part of the monies paid to Cerebral under the implied contracts to fund adequate and reasonable data security practices.

132. Plaintiff and Class Members would not have obtained mental healthcare services from Cerebral or provided and entrusted their PII and PHI to Defendant in the absence of the implied contract or implied terms between them and Cerebral. The safeguarding of the PII and PHI of Plaintiff and Class Members and prompt and sufficient notification of a breach was critical to realize the intent of the parties.

133. Plaintiff and Class Members fully performed their obligations under the implied contracts with Cerebral. Cerebral breached its implied contracts with Plaintiff and Class Members to protect their PII and PHI when it (1) failed to have security protocols and measures in place to protect that information; (2) disclosed or allowed disclosure of that information to unauthorized third parties; and (3) failed to provide timely and accurate notice to Plaintiff and Class Members that their PII and PHI was compromised as a result of the Cerebral Privacy Breach.

134. As a direct and proximate result of Cerebral's breaches of implied contract, Plaintiff and Class Members sustained actual losses and damages as described in detail above and are also entitled to recover nominal damages.

COUNT IV

Breach of Implied Covenant of Good Faith and Fair Dealing

(On behalf of Plaintiff and the Nationwide Class)

135. Plaintiff repeats and realleges all allegations set forth in paragraphs 1 through 109 above as if they were fully set forth herein.

136. Plaintiff and Class Members entered into valid, binding, and enforceable implied contracts with Cerebral, as alleged above.

137. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to

impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Cerebral would act fairly and in good faith in carrying out its contractual obligations to take reasonable measures to protect Plaintiff's and Class Members' PII and PHI and to comply with industry standards and federal and state laws and regulations.

138. A "special relationship" exists between Cerebral and the Plaintiff and Class Members. Cerebral entered into a "special relationship" with Plaintiff and Class Members who sought mental healthcare services through Cerebral and, in doing so, entrusted Cerebral, pursuant to its requirements, with their PII and PHI.

139. Despite this special relationship with Plaintiff, Cerebral did not act in good faith and with fair dealing to protect Plaintiff's and Class Members' PII and PHI.

140. Plaintiff and Class Members performed all conditions, covenants, obligations, and promises owed to Cerebral.

141. Cerebral's failure to act in good faith in implementing the security measures required by the contracts denied Plaintiff and Class Members the full benefit of their bargain, and instead they received mental healthcare and related services that were less valuable than what they paid for and less valuable than their reasonable expectations under the contracts. Plaintiff and Class Members were damaged in an amount at least equal to this overpayment.

142. Cerebral's failure to act in good faith in implementing the security measures required by the contracts also caused Plaintiff and Class Members to suffer actual damages resulting from the theft of their PII and PHI and they remain at imminent risk of suffering additional damages in the future.

143. Accordingly, Plaintiff and Class Members have been injured as a result of Cerebral's breach of the covenant of good faith and fair dealing and are entitled to damages and/or restitution in an amount to be proven at trial.

144. laintiff and Class Members that it would not disclose their PII and PHI except in a handful of clearly defined and disclosed circumstances.

145. Despite representations to the contrary, Defendant failed to protect and safeguard the PII and PHI entrusted to Cerebral by Plaintiff and Class Members and in so doing intruded on the private and personal affairs of Plaintiff and Class Members in a manner highly offensive to a reasonable person; invaded the privacy of Plaintiff and Class Members by disclosing, without authorization, the PHI and PII of Plaintiff and Class Members, inconsistent with both the purpose of the collection of the PII and PHI and inconsistent with the uses of said PII and PHI previously disclosed to Plaintiff and Class Members; failed to provide sufficient security to protect the PII and PHI of Plaintiff and Class Members from unauthorized access; enabled, by failing to protect it sufficiently, the disclosure of PII and PHI without the consent of Plaintiff or Class Members.

146. Cerebral knew, or acted with reckless disregard in not knowing, that the PII and PHI collected from Plaintiff and Class Members was, because of its nature, subject to a significant risk of unauthorized access.

147. Cerebral knew, or acted with reckless disregard in not knowing, that a reasonable person would consider its failure to adequately protect and secure their PII and PHI to be highly offensive.

148. Cerebral's disclosure of Plaintiff's and Class Members' PII and PHI without their consent constituted a violation of the privacy of Plaintiff and Class Members.

149. Cerebral's failure to provide sufficient security to protect the PII and PHI of Plaintiff and Class Members, leading to unauthorized access to that data by unauthorized parties constituted the unlawful publication of that PII and PHI by Cerebral.

150. The PII and PHI disclosed in the Cerebral Privacy Breach was not generally known to the public and is not a matter of legitimate public concern.

151. Plaintiff and Class Members had a reasonable expectation in the privacy of the PII and PHI that they provided to Cerebral. That reasonable expectation was thwarted by Defendant's actions and inactions and Defendant's conduct constituted an invasion of Plaintiff's and Class Members' privacy.

152. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial as well as restitution and injunctive relief.

153. As direct and proximate consequence of Defendant's wrongful actions, Plaintiff and Class Members have suffered the injuries alleged above.

COUNT V

Breach of Fiduciary Duty

(On behalf of Plaintiff and the Nationwide Class)

154. Plaintiff repeats and realleges all allegations set forth in paragraphs 1 through 109 above as if they were fully set forth herein.

155. Defendant accepted the special confidence placed in it by Plaintiff and Class Members, even asserting that it "use[ed] the latest information security technology to protect your data, which is not shared without your consent, and will only be used internally to improve clinical care." There was an understanding between the parties that Defendant would act for the benefit of Plaintiff and Class Members in preserving the confidentiality of the Private Information.

156. Defendant became the guardian of Plaintiff's and the Class Members' Private Information and accepted a fiduciary duty to act primarily for the benefit of its Members, including Plaintiff and the Class Members, including safeguarding Plaintiff's and the Class Members' Private Information.

157. Defendant's fiduciary duty to act for the benefit of Plaintiff and Class Members pertains as well to matters within the scope of its relationship with its Members, in particular, to keep secure the Private Information of those Members.

158. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to: (a) diligently discover, investigate, or give notice of the Privacy Breach in a reasonable and practicable period of time; (b) encrypt and otherwise protect the integrity of its computer systems containing Plaintiff's and the Class Members' Private Information; (c) timely notify and/or warn them of the Cerebral Privacy Breach; (d) ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. §164.306(a)(1); (e) implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1); (f) implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1); (g) identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. § 164.308(a)(6)(ii); (h) protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. § 164.306(a)(2); (i) protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3); (j) ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(94); (k) effectively train all members of its workforce (including independent contractors) on the policies and procedures necessary to maintain the security of PHI, in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); (l) design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in violation of 45 C.F.R. § 164.530(c); and (m) by otherwise failing to safeguard Plaintiff's and the Class Members' Private Information.

159. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and/or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Cerebral Privacy Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Cerebral Privacy Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

160. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic losses.

COUNT VI

Breach of Confidence

(On behalf of Plaintiff and the Nationwide Class)

161. Plaintiff repeats and realleges all allegations set forth in paragraphs 1 through 109 above as if they were fully set forth herein.

162. At all times during Plaintiff's and the Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Class Members' PII and PHI that Plaintiffs and the Class Members provided to Defendant.

163. As alleged herein and above, Defendant's relationship with Plaintiff and the Class Members was governed by terms and expectations that Plaintiff's and the Class Members' PII and PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

164. Plaintiff and the Class Members receiving treatment from Defendant provided Plaintiff's and the Class Members' PII and PHI to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII and PHI to be disseminated to any unauthorized third parties.

165. Plaintiff and the Class Members receiving treatment from Defendant also provided Plaintiff's and the Class Members' PII and PHI to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect that PII and PHI from unauthorized disclosure.

166. Defendant voluntarily received in confidence Plaintiff's and the Class Members' PII and PHI with the understanding that information would not be disclosed or disseminated to the public or any unauthorized third parties.

167. Due to Defendant's failure to prevent and avoid the Privacy Breach from occurring, Plaintiff's and the Class Members' PII and PHI was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Class Members' confidence, and without their express permission.

168. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Class Members have suffered damages.

169. But for Defendant's disclosure of Plaintiff's and the Class Members' PII and PHI in violation of the parties' understanding of confidence, their PII and PHI would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Privacy Breach was the direct and legal cause of the theft of Plaintiff's and the Class Members' Private Information as well as the resulting damages.

170. The injury and harm Plaintiff and the Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Class Members' PII and PHI. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Class Members' PII and PHI was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Class Members' PII and PHI.

171. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class Members, Plaintiff and the Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Privacy Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI of current and former Members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Privacy Breach for the remainder of the lives of Plaintiff and the Class Members.

///

///

///

///

COUNT VII

Declaratory Judgment

(On behalf of Plaintiff and the Nationwide Class)

172. Plaintiff repeats and realleges all allegations set forth in paragraphs 1 through 109 above as if they were fully set forth herein.

173. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

174. An actual controversy has arisen in the wake of the Privacy Breach regarding Plaintiff's and Class Members' PII and PHI and whether Cerebral is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further Privacy Breaches that compromise their PII and PHI. Plaintiff alleges that Cerebral's data security measures remain inadequate. Furthermore, Plaintiff and Class Members continue to suffer injury as a result of the compromise of their PII and PHI and remain at imminent risk that further compromises of their PII and/or PHI will occur in the future.

175. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Cerebral owes a legal duty to secure Members' PII and PHI and to timely notify Members of a Privacy Breach under the common law, Section 5 of the FTC Act and HIPAA.

b. Cerebral breached and continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI.

176. This Court also should issue corresponding prospective injunctive relief requiring Cerebral to employ adequate security protocols consistent with law and industry standards to protect Members' PII and PHI.

177. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another Privacy Breach at Cerebral. The risk of another such breach is real, immediate, and substantial. If another breach at Cerebral occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and he will be forced to bring multiple lawsuits to rectify the same conduct.

178. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Cerebral if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Cerebral of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Cerebral has a pre-existing legal obligation to employ such measures.

179. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another Privacy Breach at Cerebral, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and consumers whose confidential information would be further compromised.

COUNT VIII

Unjust Enrichment

(On behalf of Plaintiff and the Nationwide Class)

180. Plaintiff repeats and realleges all allegations set forth in paragraphs 1 through 109 above as if they were fully set forth herein.

181. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of payments made for the purchase of health care services.

182. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members.

183. The payments for mental healthcare services that Plaintiff and Class Members paid (directly or indirectly) to Defendant should have been used by

Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

184. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between the health care services with the reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and the inadequate health care services without reasonable data privacy and security practices and procedures that they received.

185. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members paid for and that were otherwise mandated by HIPAA regulations, federal, state and local laws, and industry standards.

186. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by Defendant.

187. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendant traceable to Plaintiff and Class Members.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully prays for the following relief:

A. That the Court certify this action as a class action and certify the Nationwide Class as proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper Nationwide Class representative; and appoint Plaintiff's Nationwide Counsel as Class counsel;

B. That the Court grant permanent injunctive relief to prohibit Cerebral from engaging in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and Members of the Nationwide Class compensatory, consequential, and general damages in an amount to be determined at trial;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Cerebral as a result of its unlawful acts, omissions, and practices;

E. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

F. That Plaintiff be granted the declaratory relief sought herein;

G. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

H. That the Court award pre- and post-judgment interest at the maximum legal rate; and

I. That the Court grant all such other relief as it deems just and proper.

VII. DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of the Class, hereby demands a jury trial with respect to all issues triable of right by jury.

DATED: March 17, 2023

THE WAND LAW FIRM, P.C.

By: /s/ Aubry Wand
Aubry Wand

GEORGE FELDMAN MCDONALD, PLLC
Lori G. Feldman (*pro hac vice* forthcoming)
David J. George (*pro hac vice* forthcoming)
Brittany Brown (*pro hac vice* forthcoming)

Attorneys for Plaintiff and the Putative Class